# 

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

------o0o------



**TÌM HIỂU BÀI THỰC HÀNH**

**PTIT - WINDOWS - ANALYSIS**

Giảng viên: Đinh Trường Duy

# 1. Nội dung và hướng dẫn thực hiện bài thực hành

## 1.1. Mục đích

* Giúp sinh viên có thể hiểu được cách phân tích mã độc.

## 1.2. Yêu cầu đối với sinh viên

* Có kiến thức cơ bản về hệ điều hành windows, linux, mã độc, phân tích tĩnh, phân tích động.
* Các công cụ để phân tích
* Công cụ AutoRun
* Công cụ ProcessMonitor
* Công cụ ProcessExplorer
* Công cụ IDA
* Công cụ PE studio
* Công cụ CFF Explorer
* Ngôn ngữ Python

## 1.3. Nội dung thực hành

* Link tải máy windows7 cho Vmware:

*https://ptiteduvn-my.sharepoint.com/:f:/g/personal/hieutv\_b20at063\_stu\_ptit\_edu\_vn/El7cqwVoeHRHl\_28b4Zi9tQBeayJmdPqeHDpsERyGnYt9Q?e=u00Xut*

* Khởi động bài lab:
* Vào terminal, gõ:

imodule https://github.com/NXGiang22022002/ptit-windows-analysis

*labtainer -r ptit-windows-analysis*

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

* Sau khi khởi động xong một terminal ảo sẽ xuất hiện, đại diện cho máy ptit-windows-analysis
* Sau đó thực hiện Remote vào máy windows với công cụ xfreerdp để thực hiện bài lab. Các kết quả các nhiệm vụ của sinh viên lưu vào file có tên là ATTT\_PTIT.txt để thực hiện kiểm tra hoàn thành các nhiệm vụ khi hoàn thành bài lab.
* Sinh viên làm các nhiệm vụ dưới đây để hoàn thành bài lab:
* Lưu ý: mỗi khi sử dụng 1 công cụ bất kỳ để phân tích 1 file (cả file được mã độc tạo ra để lấy thông tin hệ thống và file lưu thông tin hệ thống) cần chạy file getApp.py
* Nhiệm vụ 1: Sử dụng công cụ sshfs để chia sẻ file giữa ubuntu và windows.
* Trong máy windows 7(username: PTMD, password:1) thư mục share được lưu ở C:\Users\PTMD.WIN-5JVQ0G84U5R chứa các file: ATTT\_PTIT.txt, getApp.py.
* Trên terminal máy ptit-windows-analysis
* Sử dụng câu lệnh sau để share các file giữa windows và ubuntu:

sshfs [PTMD@IP:C:\share](mailto:PTMD@192.168.64.143:C:\share) ~/share -o nonempty,ro

* Từ máy ptit-windows-analysis dùng xfreerdp để remote sang windows7. Sử dụng câu lệnh: xfreedrp /u:username /p:password /v:IP
* Lưu ý: Nếu sshfs không thành công là do SSH trên máy windows 7 chưa hoạt động, Mở cmd.exe với quyền quản trị trên máy windows 7 và thực hiện các lệnh:
* cd C:\OpenSSH-Win64
* net start sshd
* Nhiệm vụ 2: Xác định server command and control C&C của mã độc.
* Trên máy windows, file mã độc được lưu ở Desktop có tên là tmp\_update.exe. Sử dụng Virustotal để thu thập thông tin của mã độc, lưu server command and control của mã độc vào file ATTT\_PTIT.txt. Server command and control của mã độc có dạng: http://103.168.20.12/.
* Nhiệm vụ 3: Tìm tên và nội dung của file dùng để thu thập thông tin hệ thống.
* Sử dụng công cụ IDA, phân tích mã nguồn của tmp\_update.exe để xác định các file PE được tạo ra trong quá trình thực thi.
* Tìm 2 file PE với đuôi là exe.
* Sử dụng công cụ Process Monitor để thực hiện phân tích động. Trong công cụ Process Monitor thực hiện filter process name với các file PE vừa xác định được ở trên. Chạy công cụ Process Monitor để giám sát.
* Tiến hành chạy mã độc.
* Đọc dữ liệu thu được và xác định đường dẫn và tên file được mã độc tạo ra và lưu vào file ATTT\_PTIT.txt (2 file PE với đuôi là exe, 1 file được mã độc tạo ra để lấy thông tin hệ thống, 1 file lưu thông tin hệ thống).
* Lưu nội dung file .bat có thể đọc được vào file ATTT\_PTIT.txt. Mở file được mã độc tạo ra để lấy thông tin hệ thống và file lưu thông tin hệ thống(victim.txt), sau đó chạy getApp.py.

+ Nhiệm vụ 4: Xác định mã độc có duy trì truy cập trên hệ thống không?

* Thực hiện xóa file lưu thông tin của hệ thống đã tìm được ở nhiệm vụ trước và khởi động lại hệ thống. Sau đó truy cập vào thư mục chứa file lưu thông tin hệ thống vừa xóa thì thấy lại chứa file lưu thông tin hệ thống vẫn tức là mã độc đã thực hiện hành vi duy trì truy cập trên hệ thống, ngược lại nếu không tìm thấy thì mã độc không thực hiện hành vi duy trì truy cập trên hệ thống.
* Nếu mã độc thực hiện hành vi duy trì truy cập trên hệ thống, chạy công cụ AutoRun để xác định mã độc thực hiện hành vi duy trì truy cập trên hệ thống bằng cách nào và lưu đầy đủ đường dẫn, name và data của key mã độc đã tạo vào file ATTT\_PTIT.txt.
* Nhiệm vụ 5: Xác định địa chỉ bắt đầu thực thi của tmp\_update.exe.
* Sử dụng công cụ CFF Explorer để xác định giá trị của AddressOfEntryPoint và Import Directory RVA của file tmp\_update.exe và lưu vào file ATTT\_PTIT.txt.
* Nhiệm vụ 6: Xác định tên và đường dẫn của file PE từ resource đã bị mã độc drop.
* Sử dụng công cụ IDA để phân tích các tất cả các hàm qua đó xác định hành vi của mã độc. Lưu tên Resource và file PE vào file ATTT\_PTIT.txt (viết số hệ thập phân).
* Nhiệm vụ 7: Xác định thuật toán mã hóa mà mã độc sử dụng để mã hóa dữ liệu và KEY của thuật toán mã hóa?
* Sử dụng công cụ IDA để phân tích mã nguồn các file PE và xác định thuật toán mã độc sử dụng để mã hóa là gì? (AES, A5/1, RSA, RC4, DES, 3DES, …) Ghi tên thuật toán mã hóa vào file ATTT\_PTIT.txt.
* Sử dụng công cụ CFF Explorer để xác định giá trị KEY mã độc sử dụng trong quá trình mã hóa? (KEY là mã hex có dạng 76 83 89 ….) Ghi KEY vào file ATTT\_PTIT.txt.
* Nhiệm vụ 8: Thực hiện giải mã Resoure 107 đã bị mã hóa.
* Mở trình duyệt, truy cập vào trang web: [*https://gchq.github.io/CyberChef/*](https://gchq.github.io/CyberChef/) sử dụng công cụ CyberChef để giải mã. Lưu bản rõ đã giải mã từ resource 107 vào file ATTT\_PTIT.txt.
* Nhiệm vụ 9: Xác định mã độc có thực hiện các kỹ thuật anti reverse, anti debug, antiVM hay không?
* Sử dụng công cụ IDA phân tích mã nguồn các file PE mã độc đã tạo ra để xác định các kỹ thuật anti mà mã độc sử dụng.
* Nếu mã độc sử dụng kỹ thuật anti reverse, anti debug, antiVM thì lưu cách mã độc sử dụng kỹ thuật đó, giá trị key (nếu có) vào file ATTT\_PTIT.txt
* Để thực hiện checkwork các nhiệm vụ sinh viên sử dụng lệnh cat file ATTT\_PTIT.txt và log.txt.
* Sau đó, sinh viên kết nối đến 1 container khác thông qua ssh bằng lệnh sau:

*ssh* [*ubuntu@172.17.0.x(1-10)*](mailto:ubuntu@172.17.0.x(1-10))

* Mật khẩu chính là thuật toán mã hóa mà sinh viên vừa tìm được ở bước trên. Tiếp theo, sinh viên hãy in ra màn hình tệp tin filetoview:

*cat filetoview.txt*

* Kết thúc bài lab:
* Trên terminal đầu tiên sử dụng câu lênh sau để kết thúc bài lab:

*stoplab ptit-windows-analysis*

* Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.
* Khởi động lại bài lab:
* Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*labtainer -r ptit-windows-analysis*